PhoneCentral.io
Communicate. Collaborate. Create.

Robocall Mitigation Plan

PhoneCentral.io | A DBA of Swiftcom Tech LLC | UCaaS Voice Services

SERVICE MODEL	OPERATING BRAND	FOUNDER & DIRECTOR
Cloud UCaaS / VoIP	PhoneCentral.io	Adnan Patni

01 PURPOSE & SCOPE

Swiftcom Tech LLC DBA PhoneCentral.io ("PhoneCentral.io") provides cloud business phone systems and contact-center communications, including inbound and outbound VoIP calling, call routing, and related messaging services. This plan addresses illegal robocall risks associated with voice traffic originated through its platform and interconnected carrier relationships.

PhoneCentral.io applies a **prevent, detect, and mitigate** approach designed to protect consumers, preserve legitimate business communications, and support applicable FCC robocall mitigation obligations.

02 PREVENTION & CUSTOMER SCREENING

- **Business verification.** Collect and review the customer's legal business identity, responsible contact, business purpose, and intended call use case before enabling outbound voice access.
- **Caller-ID authorization.** Require customers to use telephone numbers they own, control, or are specifically authorized to present. Restrict spoofed, invalid, and misleading caller ID.
- **Risk-based onboarding.** Review high-risk calling uses and suspicious account details; request additional supporting records or decline service when risks cannot be resolved.
- **Compliance terms.** Prohibit unlawful automated calling, fraud, misleading identity, and calling without legally required consent; require compliance with TCPA, Do Not Call rules, and applicable law.
- **Carrier and provider checks.** Review relevant interconnection partners and, where applicable, verify upstream or wholesale providers in the FCC Robocall Mitigation Database.

Technical & Operational Controls

Steps used to authenticate, monitor, and assess outbound voice traffic

03 CALLER ID & STIR/SHAKEN

PhoneCentral.io maintains controls to link outbound calls to customer accounts and their approved caller IDs. Calls route through authorized PSTN interconnection partners; STIR/SHAKEN authentication is performed by PhoneCentral.io and/or an authorized originating partner **as applicable to the actual call path**. Attestation is based on verified customer identity, number authorization, and the relevant signing arrangement.

- Do not assume that a customer-provided number qualifies for a particular STIR/SHAKEN attestation level merely because it appears in the caller-ID field.
- Investigate unauthorized caller-ID substitutions, caller-ID rotation, and traffic inconsistent with the customer's approved use case.

04 MONITORING & DETECTION

PhoneCentral.io reviews call-detail records, account activity, customer reports, and interconnecting-carrier notifications to identify potential illegal calling activity. Monitoring may consider:

- **Volume anomalies:** abrupt traffic spikes, unusually high call rates, or repeated short-duration calls.
- **Call outcomes:** abnormal rejection patterns, repeated calls to the same destinations, or indicators of unwanted traffic.
- **Identity and complaint signals:** frequent caller-ID changes, suspected spoofing, fraud complaints, or traceback referrals.

Potential concerns are escalated for review, using available SIP signaling records, CDRs, customer records, and information shared by carrier partners. Any third-party analytics arrangements must be described accurately in the FCC filing when applicable.

05 NETWORK & ACCOUNT SAFEGUARDS

- Limit outbound calling privileges to approved customer accounts and authorized user credentials.
- Use appropriate account restrictions, caller-ID controls, traffic limits, and service suspension capabilities to reduce abuse.
- Keep reasonable records linking call activity to a customer, service account, originating number, and relevant timestamp.

Mitigation & Accountability

Complaint response, traceback cooperation, and program governance

06 RESPONSE TO SUSPECTED ILLEGAL CALLING

1. **Identify:** Review complaints, unusual traffic patterns, carrier alerts, or law-enforcement reports.
2. **Investigate:** Trace the activity to the customer account, caller ID, time window, and relevant CDRs; seek a customer explanation where appropriate.
3. **Contain:** Apply proportionate restrictions, rate limits, number blocking, or temporary suspension to stop suspected unlawful traffic.
4. **Resolve:** Require corrective action, monitor recurrence, and terminate access when violations are confirmed or material risks persist.

07 TRACEBACK & COOPERATION

PhoneCentral.io is committed to responding **fully and within 24 hours** to traceback requests from the FCC, law enforcement, and the designated industry traceback consortium. It will cooperate in identifying the source of illegal calls, share responsive records through appropriate channels, and coordinate promptly with its customers and carrier partners to stop unlawful traffic.

08 OVERSIGHT & RECORDS

The Founder and Director oversees implementation of this program and escalation of material incidents. Customer-verification records, call logs, complaints, investigations, and mitigation actions are retained under applicable law and company recordkeeping procedures. The plan is reviewed periodically and updated when operations, risks, or FCC requirements change.

RESPONSIBLE OFFICER

Adnan Patni

Founder and Director | Swiftcom Tech LLC (DBA PhoneCentral.io)

Regulatory framework: 47 CFR § 64.6305 and related FCC requirements, as applicable.